

Figure 1

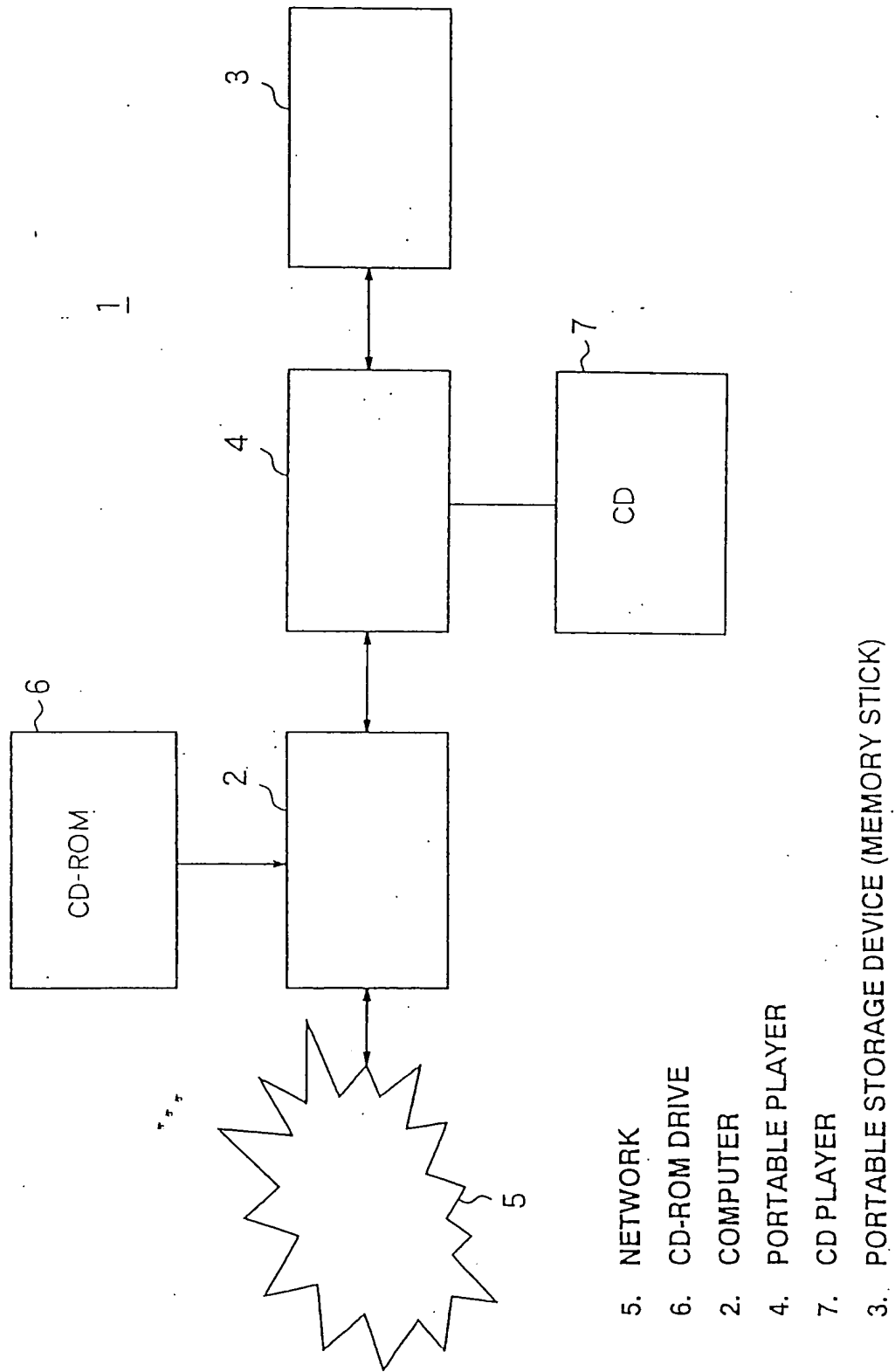
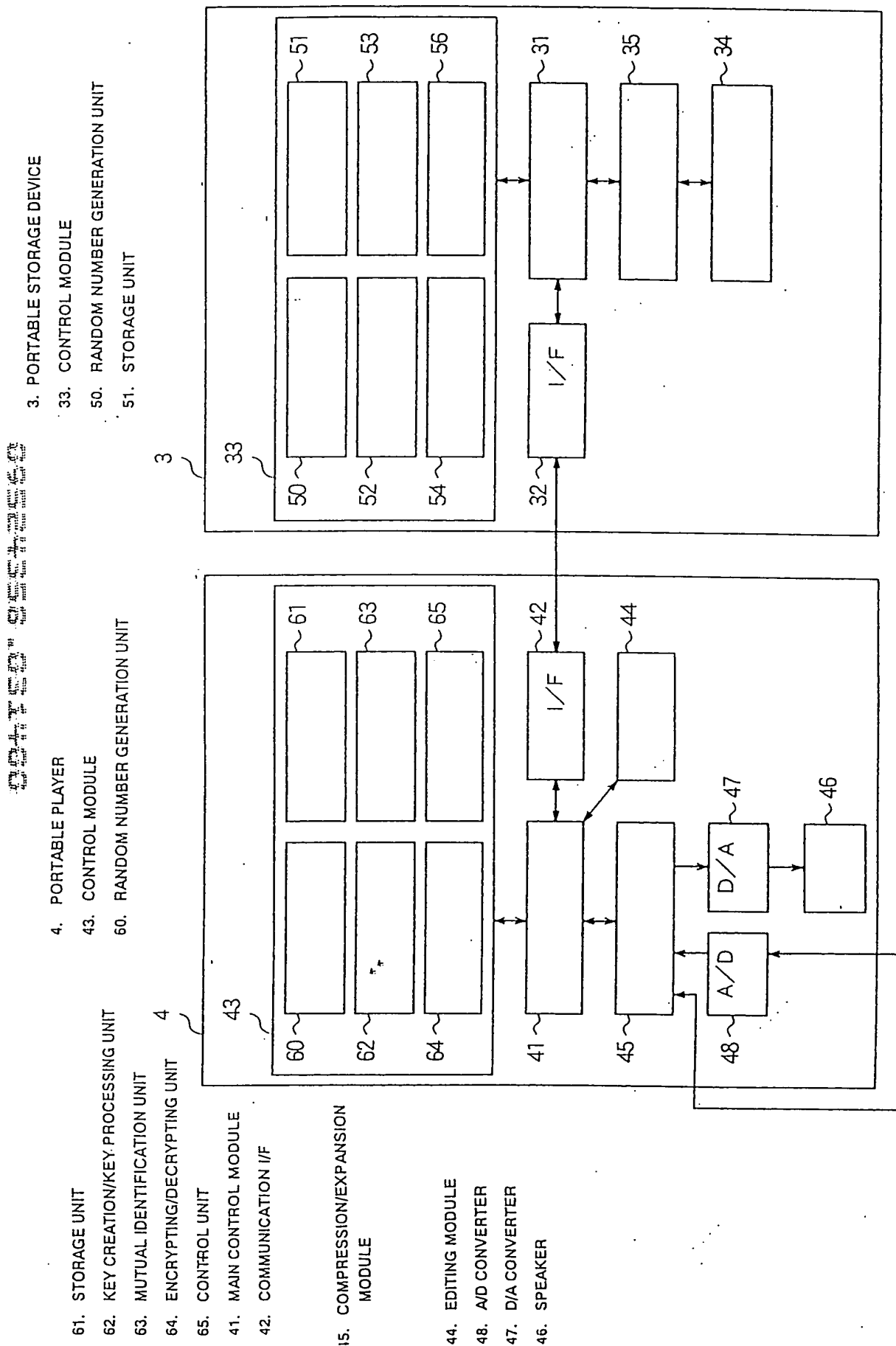


Figure 2



- 52. KEY CREATION/KEY PROCESSING UNIT
- 53. MUTUAL IDENTIFICATION UNIT
- 54. ENCRYPTING/DECRYPTING UNIT
- 55. CONTROL UNIT
- 32. COMMUNICATION I/F
- 31. MAIN CONTROL MODULE
- 35. FLASH MEMORY MANAGEMENT MODULE

AUDIO DATA (FROM COMPUTER 2) AUDIO DATA (FROM CD PLAYER 7)

Figure 3

DATA STORED IN STORAGE UNIT 51 OF PORTABLE STORAGE DEVICE 3

IDENTIFICATION KEY DATA

$I K_0$

$I K_1$

$I K_2$

$I K_3$

\vdots

$I K_{30}$

$I K_{31}$

DEVICE IDENTIFICATION DATA

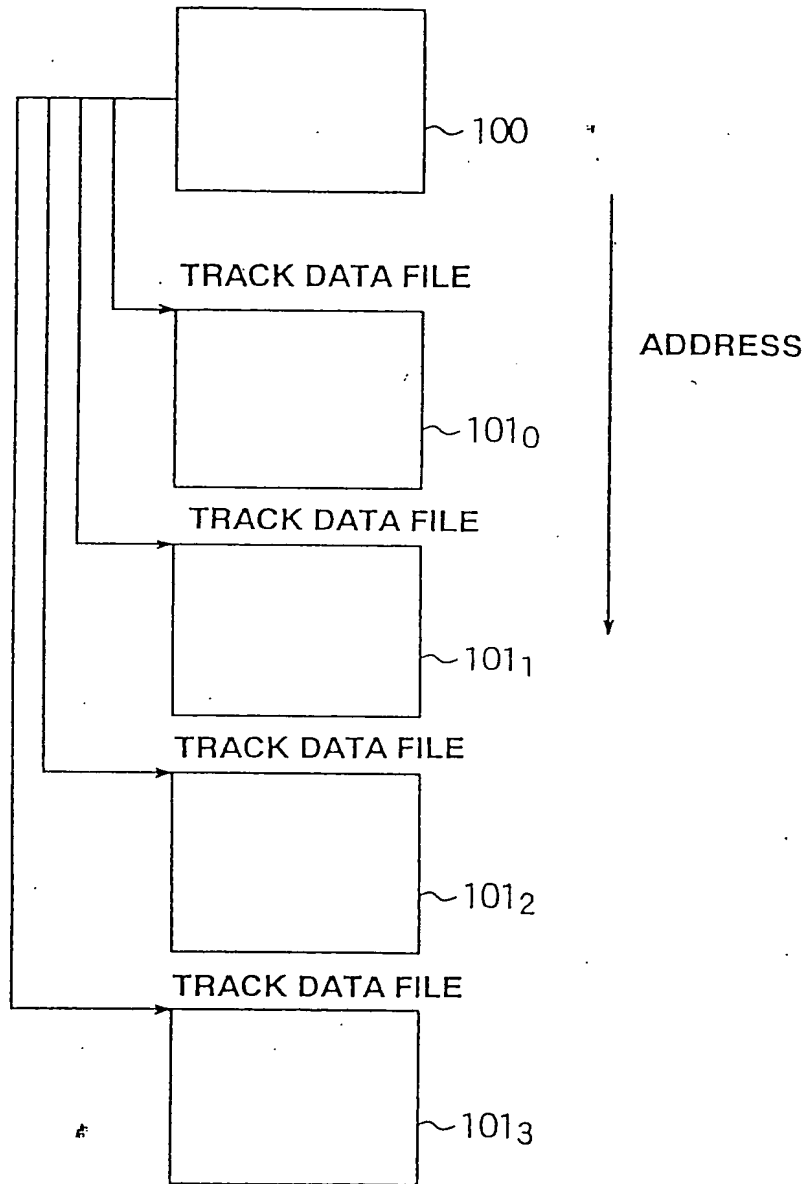
$I D_m$

STORAGE USE KEY DATA

SK_m

Figure 4

REPRODUCTION MANAGEMENT FILE



STORAGE DATA OF FLASH MEMORY 34 OF PORTABLE STORAGE DEVICE 3

Figure 5

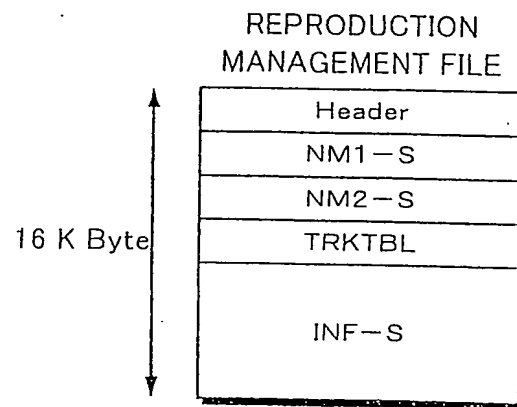


Figure 6

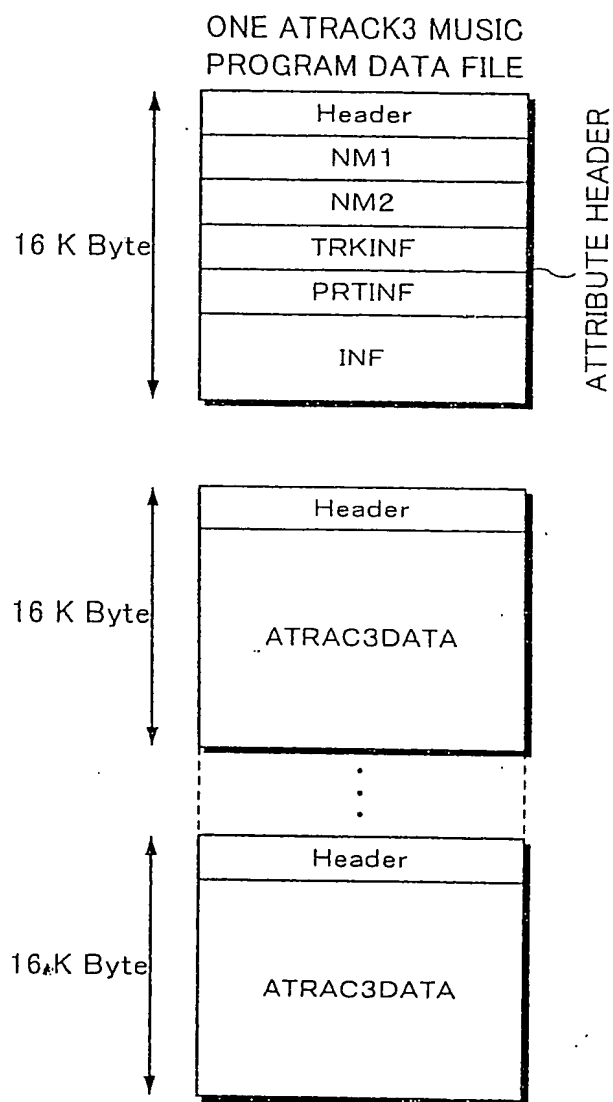


Figure 7

REPRODUCTION MANAGEMENT FILE

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0X0000	BLKID-TLO			Reserved	MCode	REVISION			Reserved							
0X0010	SN1C+L		SN2C+L	SINFSIZE	T-TRK	VerNo			Reserved							
0X0020	NM1-S(256)															
0X0120	NM2-S(512)															
0X0320	Reserved				CONTENTSKY											
0X0330	Reserved				MAC											
0X0350	Reserved				S-YMDhms											
	TRK-001	TRK-002	TRK-003	TRK-004	TRK-005	TRK-006	TRK-007	TRK-008								
	TRK-009	TRK-010	TRK-011	TRK-012	TRK-013	TRK-014	TRK-015	TRK-016								
0X0660	TRK-393	TRK-394	TRK-395	TRK-396	TRK-397	TRK-398	TRK-399	TRK-400								
0X0647	INF-S(14720)															
0X3FF0	BLKID-TLO			Reserved	MCode	REVISION			Reserved							

TRKTB L

1. *What is the main purpose of the text?*
 2. *What are the key points discussed in the text?*
 3. *What are the main arguments presented?*
 4. *What are the main conclusions drawn?*
 5. *What are the main recommendations made?*
 6. *What are the main findings of the study?*
 7. *What are the main implications of the study?*
 8. *What are the main limitations of the study?*
 9. *What are the main strengths of the study?*
 10. *What are the main weaknesses of the study?*
 11. *What are the main contributions of the study?*
 12. *What are the main limitations of the study?*
 13. *What are the main strengths of the study?*
 14. *What are the main weaknesses of the study?*
 15. *What are the main contributions of the study?*

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
INF	0x00	ID	0x00	SIZE	MCode	C+L	Reserved	DATA VARIABLE LENGTH							

Figure 9

TRACK DATA FILE

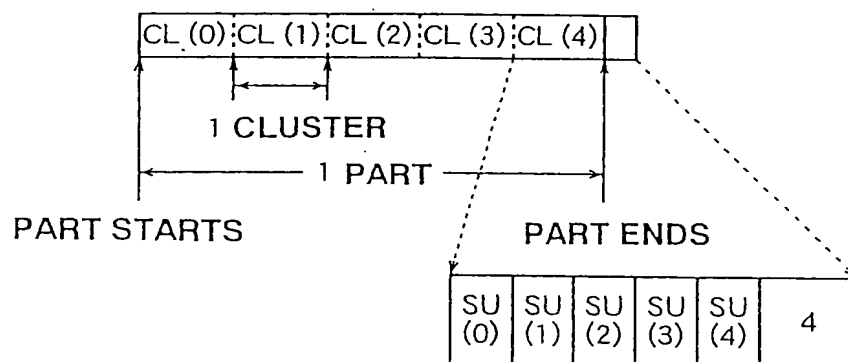


Figure 10

A3Dnnnnn.MSA(ATRAC3 DATA FILE)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID-HD0			Reserved		MCode		Reseved			BLOCK SERIAL					
0x0010	N1C+L		N2C+L		INFSIZE		T-PRT		T-SU			INX		XT		
0x0020	NM1(256)															
0x0120	NM2(512)															
0x0310																
0x0320	Reserved(8)								CONTENTSKEY							
	Reserved(8)								MAC							
	Reserved(12)												A	LT	FNo	
	MG(D)SERIAL-nnn															
	CONNUM				YMDhms-S				YMDhms-E				MT	CT	CC	CN
	PRTSIZE				PRTKEY								Reserved(8)			
0x0360	CONNUM				YMDhms-S				YMDhms-E				MT	CT	CC	CN
0x0370	PRTSIZE				PRTKEY								Reserved(8)			
0x0380					CONNUM0				PRTSIZE(0x0388)				PRTKEY			
0x0390					Reserved(8)								CONNUM0			
	INF(0x0400)															
0x3FFF	BLKID-HD0			Reserved		MCode		Reseved			BLOCK SERIAL					
0x4000	BLKID-A3D			Reserved		MCode		CONNUM0			BLOCK SERIAL					
0x4010	BLOCK SEED								INITILIZATION VECTOR							
0x4020	SU-000(Nbyte=384byte)															
0x41A0	SU-001(Nbyte)															
0x4320	SU-002(Nbyte)															
0x04A0	SU-041(Nbyte)															
0x7DA0	Reserved(Nbyte=208byte)															
0x7F20																
	BLOCK SEED															
0x7FF0	BLKID-A3D			Reserved		MCode		CONNUM0			BLOCK SERIAL					

Figure 11

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID-HD0				Reserved		MCode		Reseved				BLOCK SERIAL			
0x0010	N1C+L		N2C+L		INFSIZE		T-PRT		T-SU				INX		XT	
0x0020	NM1(256)															
0x0120	NM2(512)															
0x0310																

Figure 12

0x0320	Reserved(8)				CONTENTSKEY					
	Reserved(8)				MAC					
	Reserved(12)				A	LT	FNo			
	MG(D)SERIAL- <i>nnn</i>									
0x0360	CONNUM		YMDhms-S		YMDhms-E		MT	CT	CC	CN

Figure 13

bit7:MODE OF ATRAC3 0: Dual 1: Joint

bit6,5,4 N OF 3 BITS:MODE VALUE

N	MODE	TIME	TRANSMISSION RATE	SU	BYTES
7	HQ	47min	176kbps	31SU	512
6		58min	146kbps	38SU	424
5	EX	64min	132kbps	42SU	384
4	SP	81min	105kbps	53SU	304
3		90min	94kbps	59SU	272
2	LP	128min	66kbps	84SU	192
1	mono	181min	47kbps	119SU	136
0	mono	258min	33kbps	169SU	96

bit3:Reserved

bit2:DATA TYPE 0:AUDIO 1:OTHER

bit1:REPRODUCTION SKIP 0:NORMAL REP 1:SKIP

bit0:EMPHASIS 0:OFF 1:ON(50/15 μ S)

Figure 14

bit7	:COPY PERMISSION	0:COPY PROHIBITION	1:COPY PERMISSION
bit6	:GENERATION	0:ORIGINAL	1:FIRST OR LATER COPY GENERATION
HCMS bit5-4	:COPY CONTROL FOR HIGH SPEED DIGITAL COPY		
	00:COPY PROHIBITION 01:COPY FIRST GENERATION 10:COPY PERMISSION		
	COPY OF FIRST COPY GENERATION IS PROHIBITED.		
bit3-2	MagicGate AUTHENTICATION LEVEL		
	00:Level10(Non-MG)	01:Level1	
	10:Level2	11:Reserved	
	DIVIDE AND COMBINE ARE PROHIBITED IN OTHER THAN LEVEL 10.		
bit1,0	Reserved		

Figure 15

0x0370	PRTSIZE	PRTKEY		Reserved(8)
0x0380		CONNUM0	PRTSIZE(0x0388)	PRTKEY
0x0390		Reserved(8)		CONNUM0

Figure 16

0x4000	BLKID-A3D	Reserved	MCode	CONNUM0	BLOCK SERIAL
0x4010	BLOCK SEED			INITIALIZATION VECTOR	
0x4020	SU-000(Nbyte=384byte)				

Figure 17

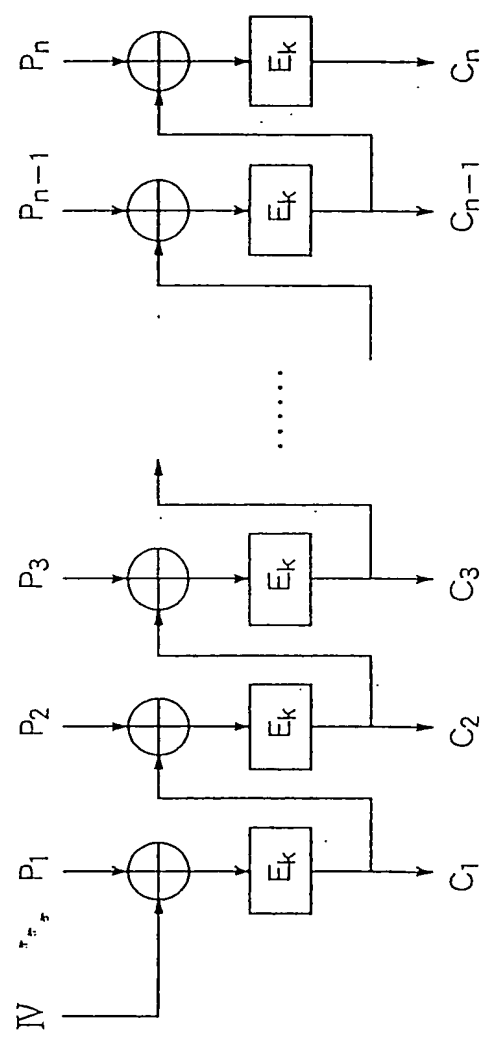
DATA TO BE STORED IN STORAGE UNIT 61 OF PORTABLE PLAYER 4

	MK ₀
MASTER KEY DATA	MK ₁
	MK ₂
	MK ₃
	⋮
	MK ₃₀
	MK ₃₁
DEVICE IDENTIFICATION DATA	I D _d

Figure 18

DES CBC MODE (ENCRYPTION)

$$C_i = E_k (P_i \oplus C_{i-1})$$

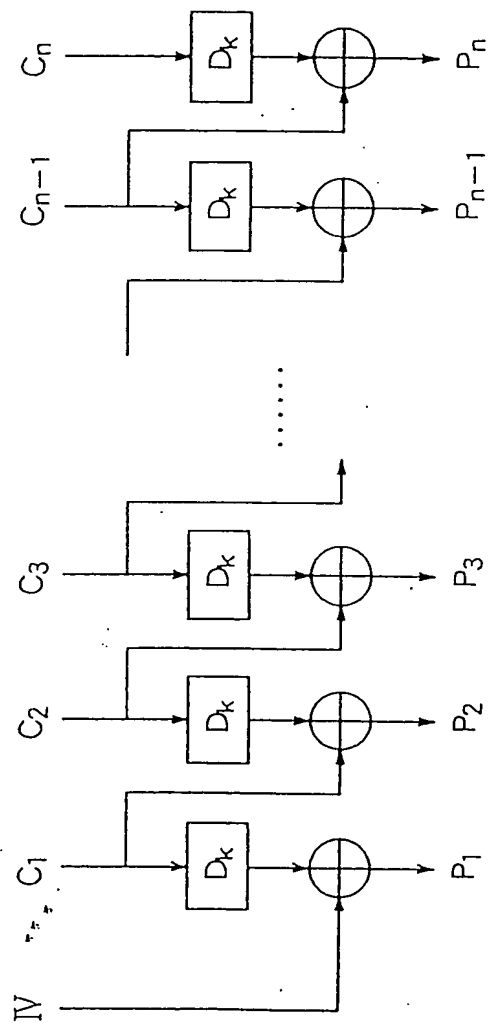


- IV : Initialization Vector
- P_i : Plaintext
- C_i : Ciphertext
- E_k : DES encipherment with key k

Figure 19

DES CBC MODE (DECRYPTION)

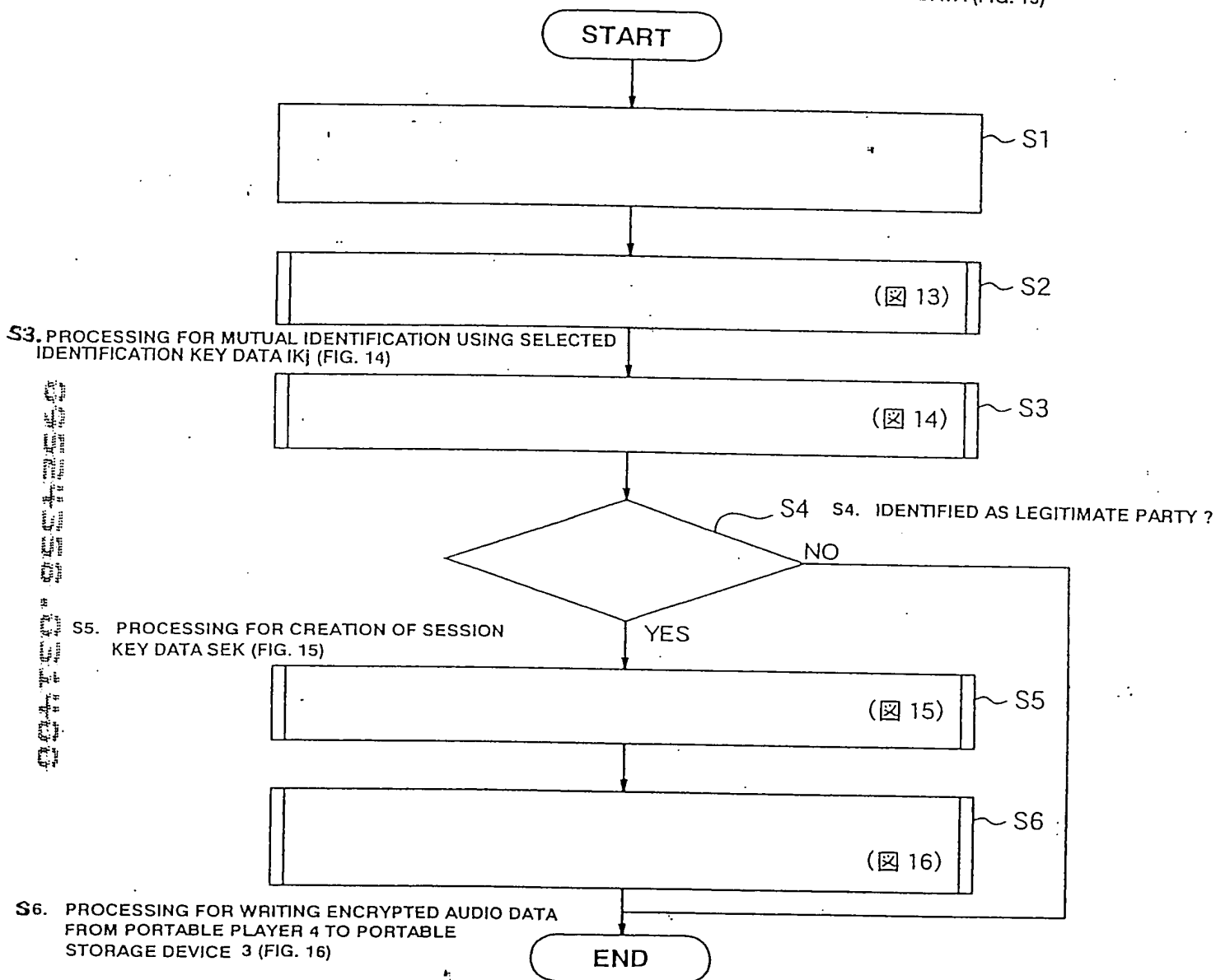
$$P_i = C_{i-1} \text{ XOR } D_k(C_i)$$



- IV : Initialization Vector
- P_i : Plaintext
- C_i : Ciphertext
- D_k : DES decipherment with key k

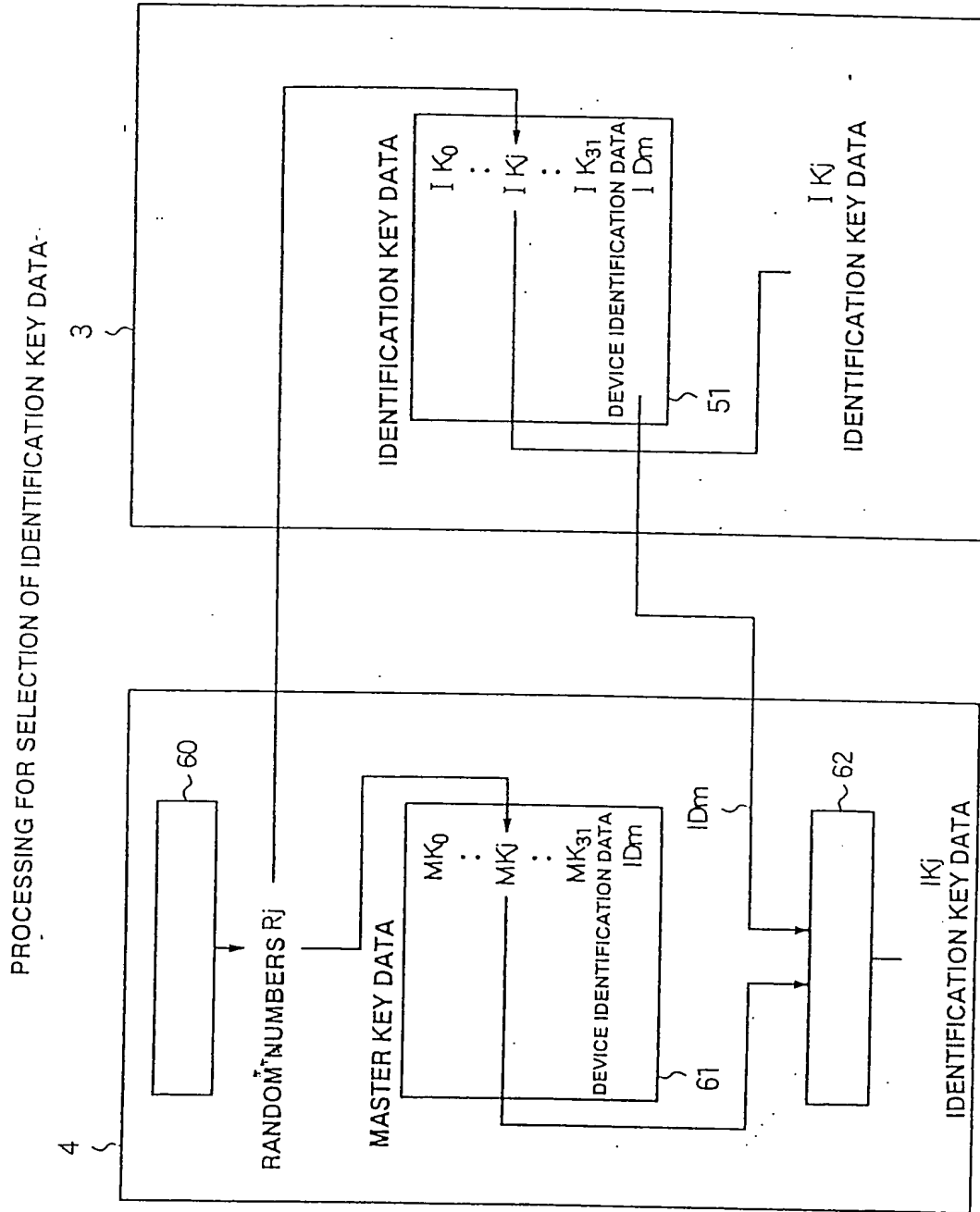
Figure 20

- S1. OUTPUT WRITE REQUEST SIGNAL FROM PORTABLE PLAYER 4 TO PORTABLE STORAGE DEVICE 3
 S2. PROCESSING FOR SELECTION OF IDENTIFICATION KEY DATA (FIG. 13)



WRITE PROCESSING TO PORTABLE STORAGE DEVICE 3

Figure 21



60. RANDOM NUMBER GENERATION UNIT

61. STORAGE UNIT

62. KEY CREATION PROCESSING UNIT

51. STORAGE UNIT

Figure 22

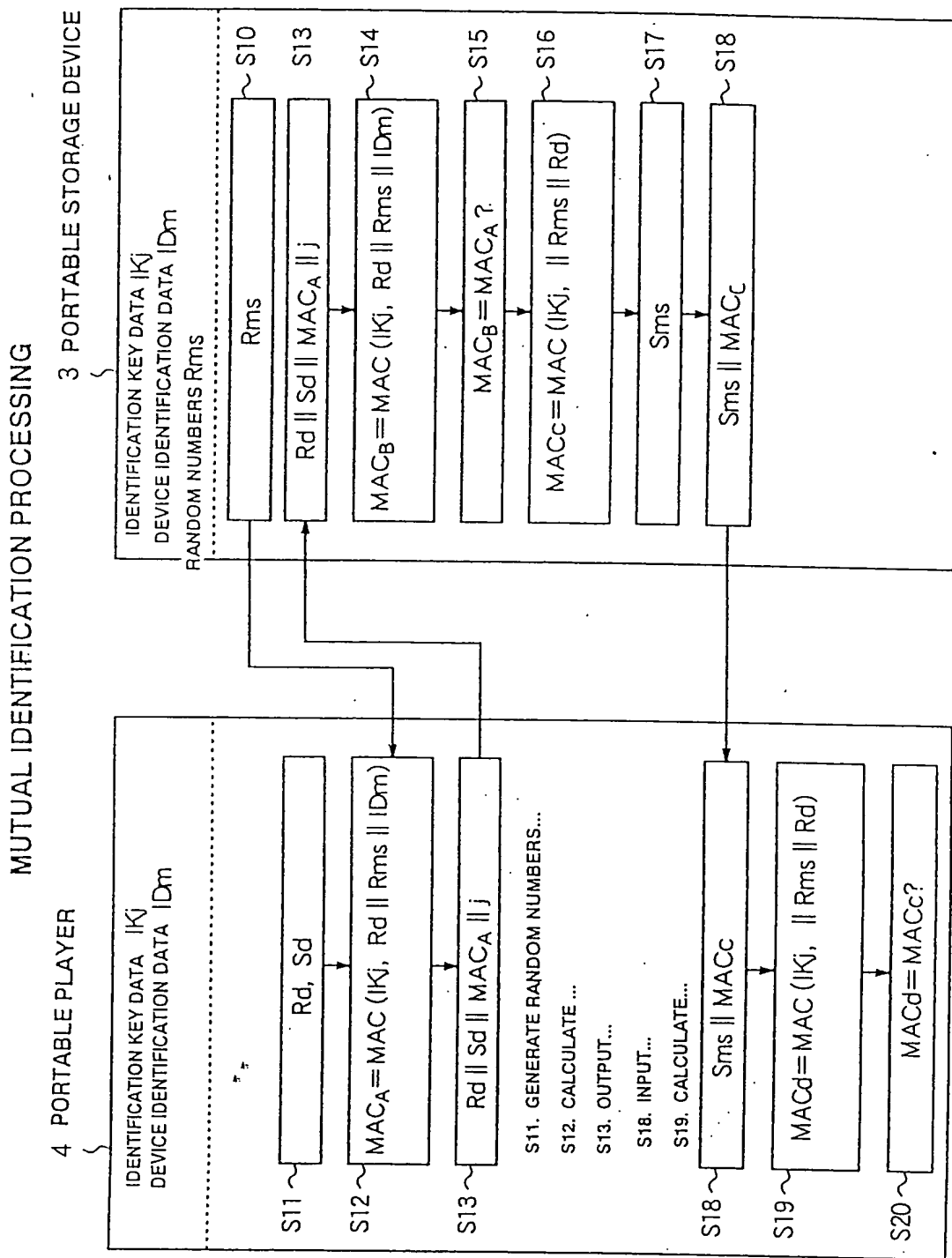


Figure 23

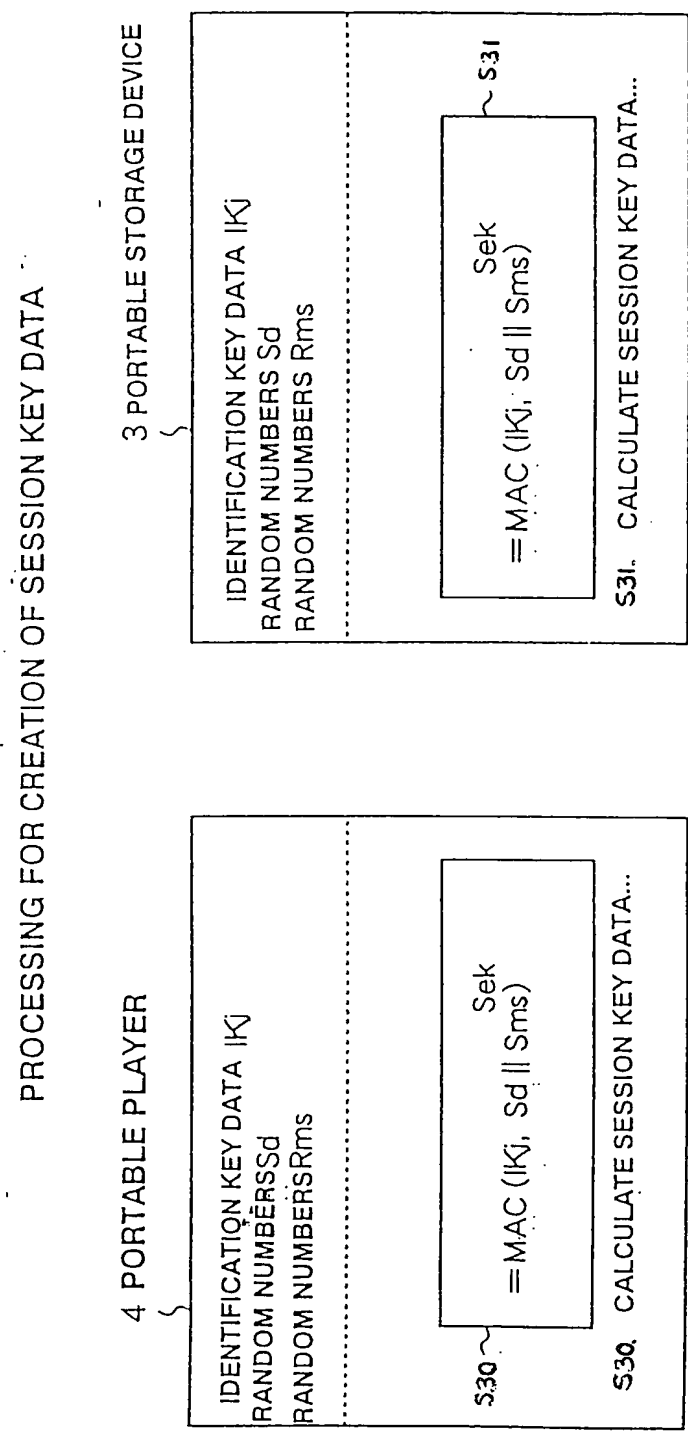


Figure 24

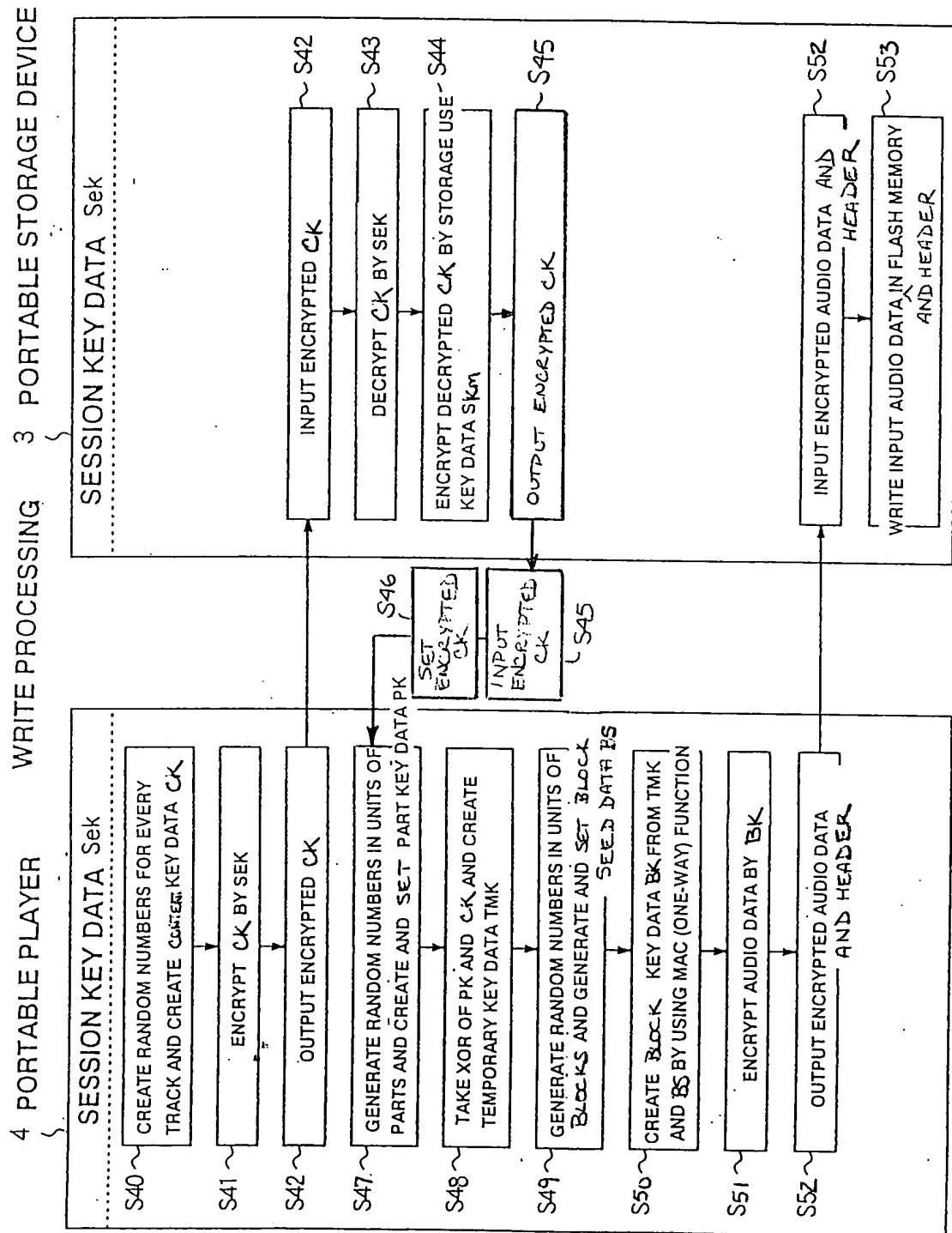
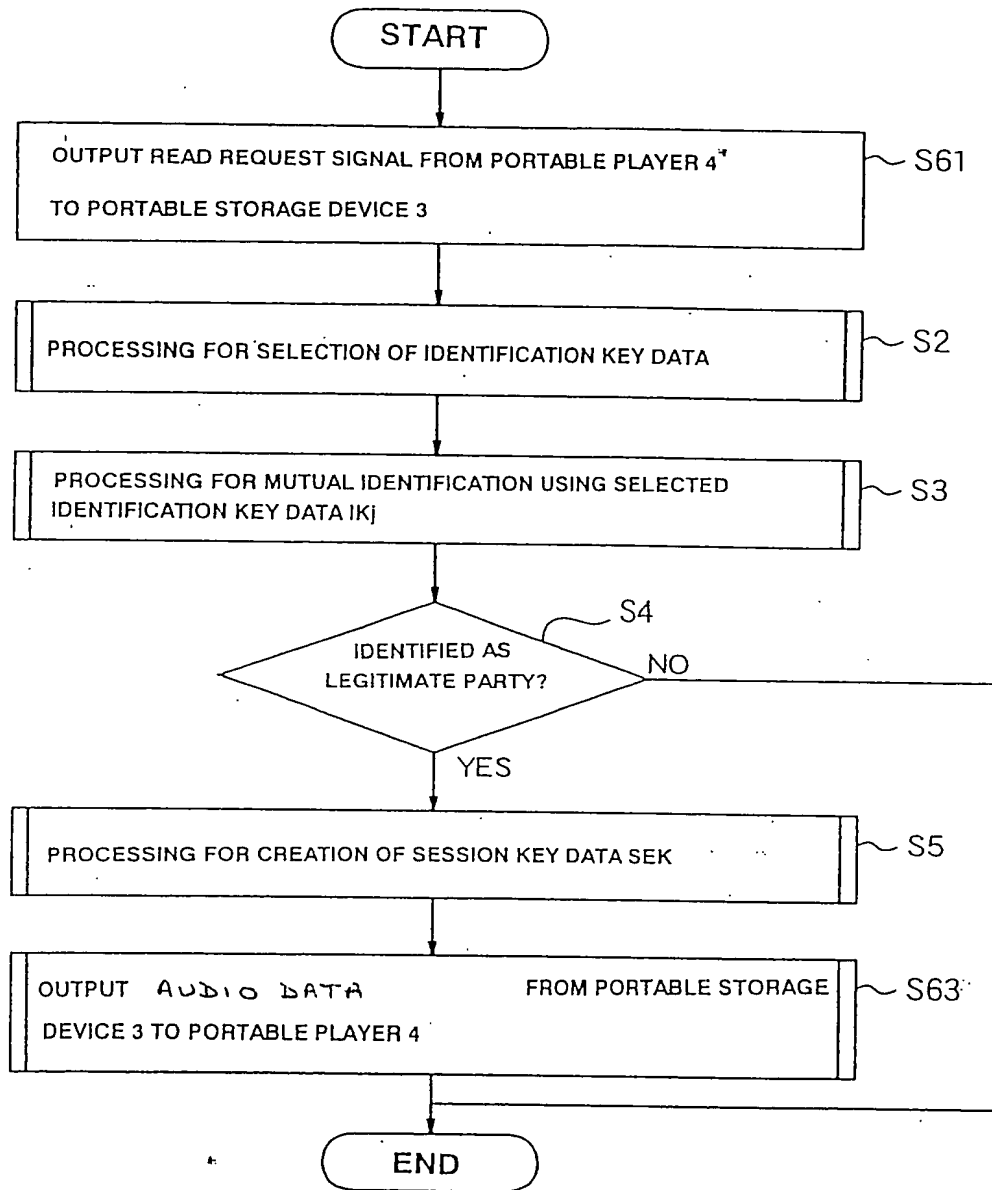


Figure 25



PROCESSING FOR READING FROM PORTABLE STORAGE DEVICE 3

Figure 26

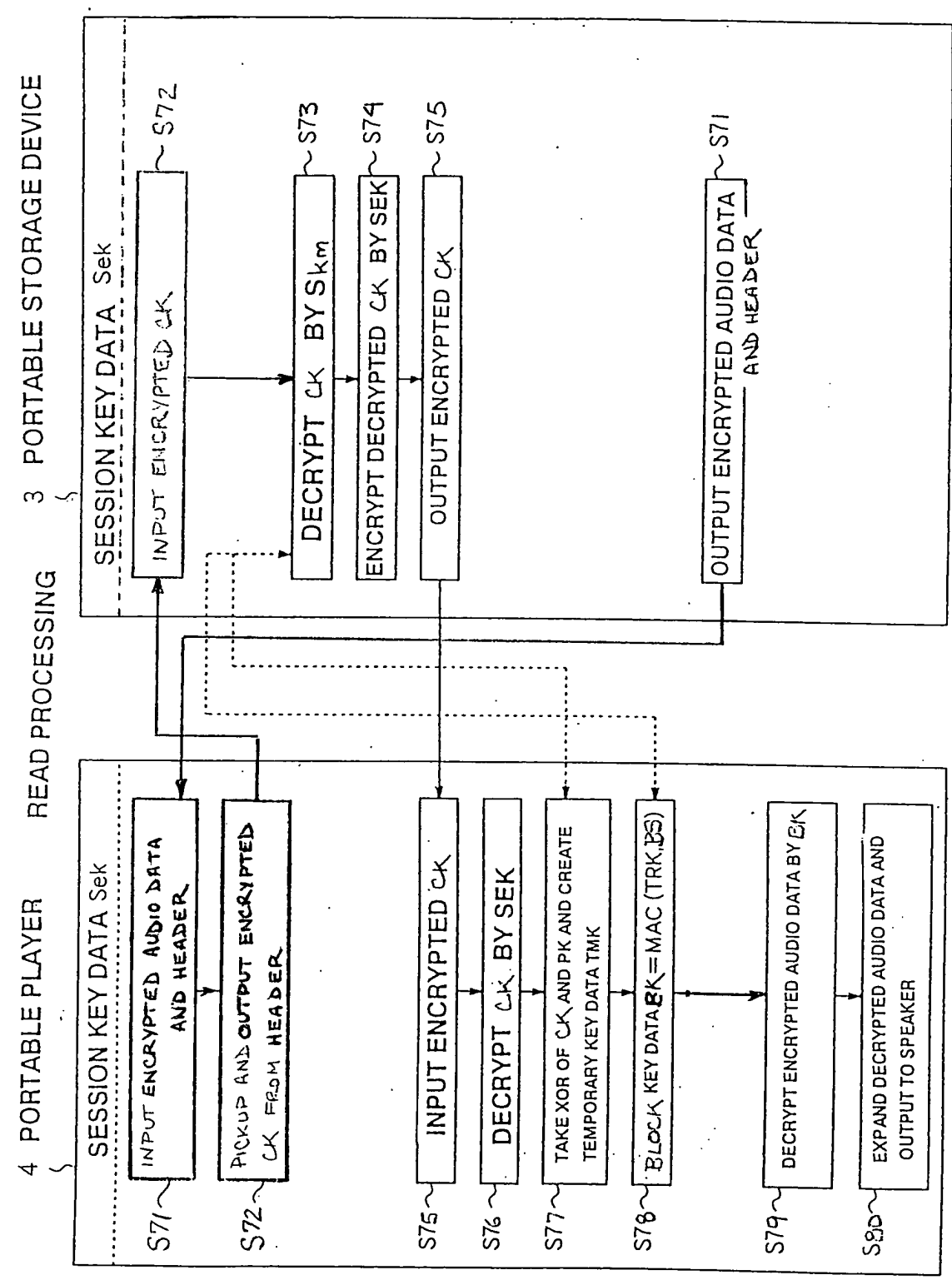


Figure 27

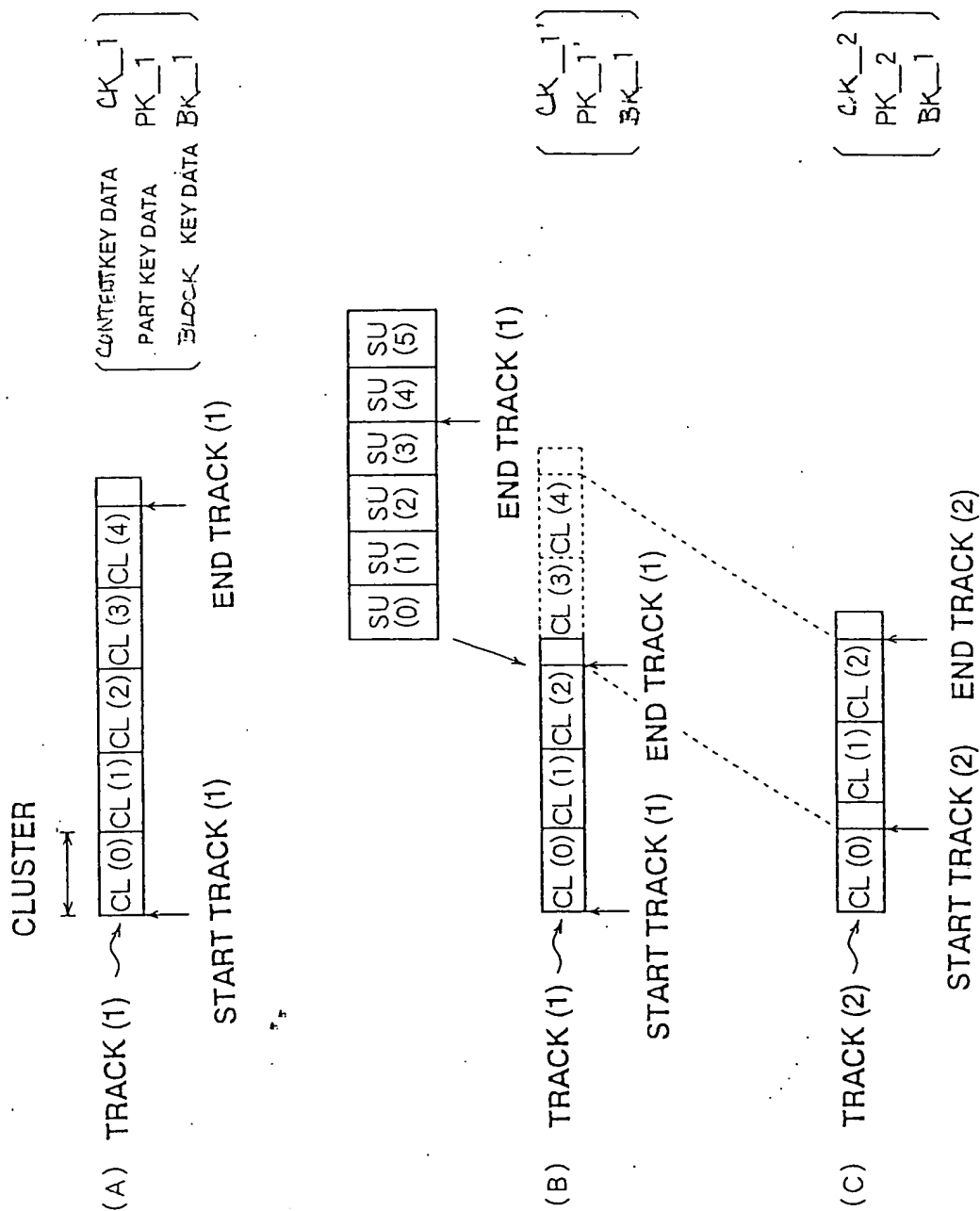


Figure 28

Cluster CL(2) of Track(1) after divide

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
Address ↓	BLKID-A3D			Reserved			MCode			CONNUM0				BLOCK SERIAL			
	BLOCK SEED									INITIALIZATION VECTOR (last 8 bytes of last SU of CL(1))							
	SU(0)																
	SU(1)																
	SU(2)																
	SU(3)																
	BLOCK SEED																
BLKID-A3D			Reserved			MCode			CONNUM0				BLOCK SERIAL				

Address



Figure 29

Cluster CL(0) of Track(2) after divide

0 1 2 3 4 5 6 7 8 9 A B C D E F															
BLKID-A3D			Reserved			MCode			CONNUM0				BLOCK SERIAL		
BLOCK SEED								INITIALIZATION VECTOR (last 8 bytes of last SU(3) of CL(2) of track(1))							
SU(0) (SU(4) of CL(2) of original track(1))															
SU(1) (SU(5) of CL(2) of original track(1))															

Address



Figure 30

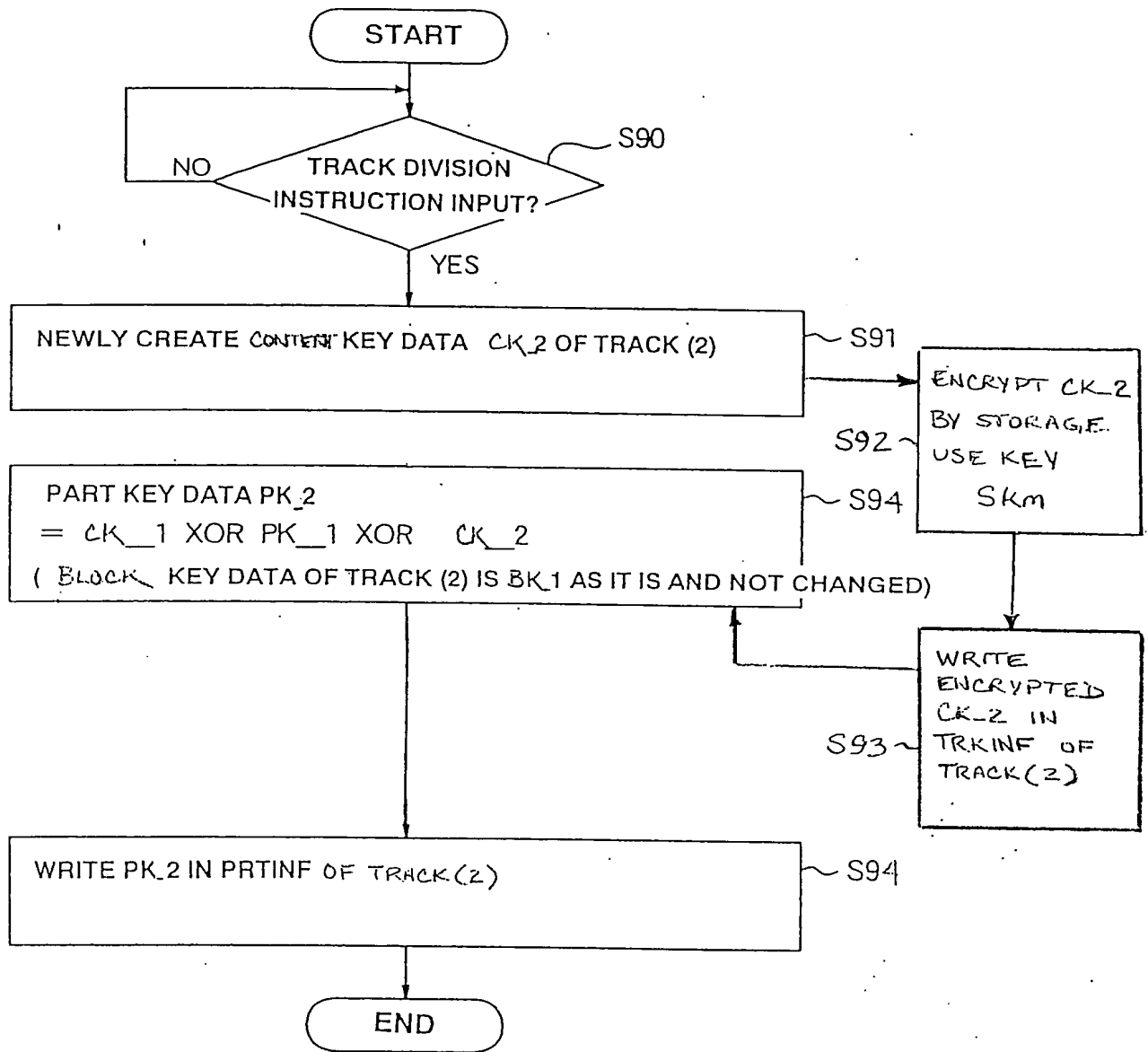
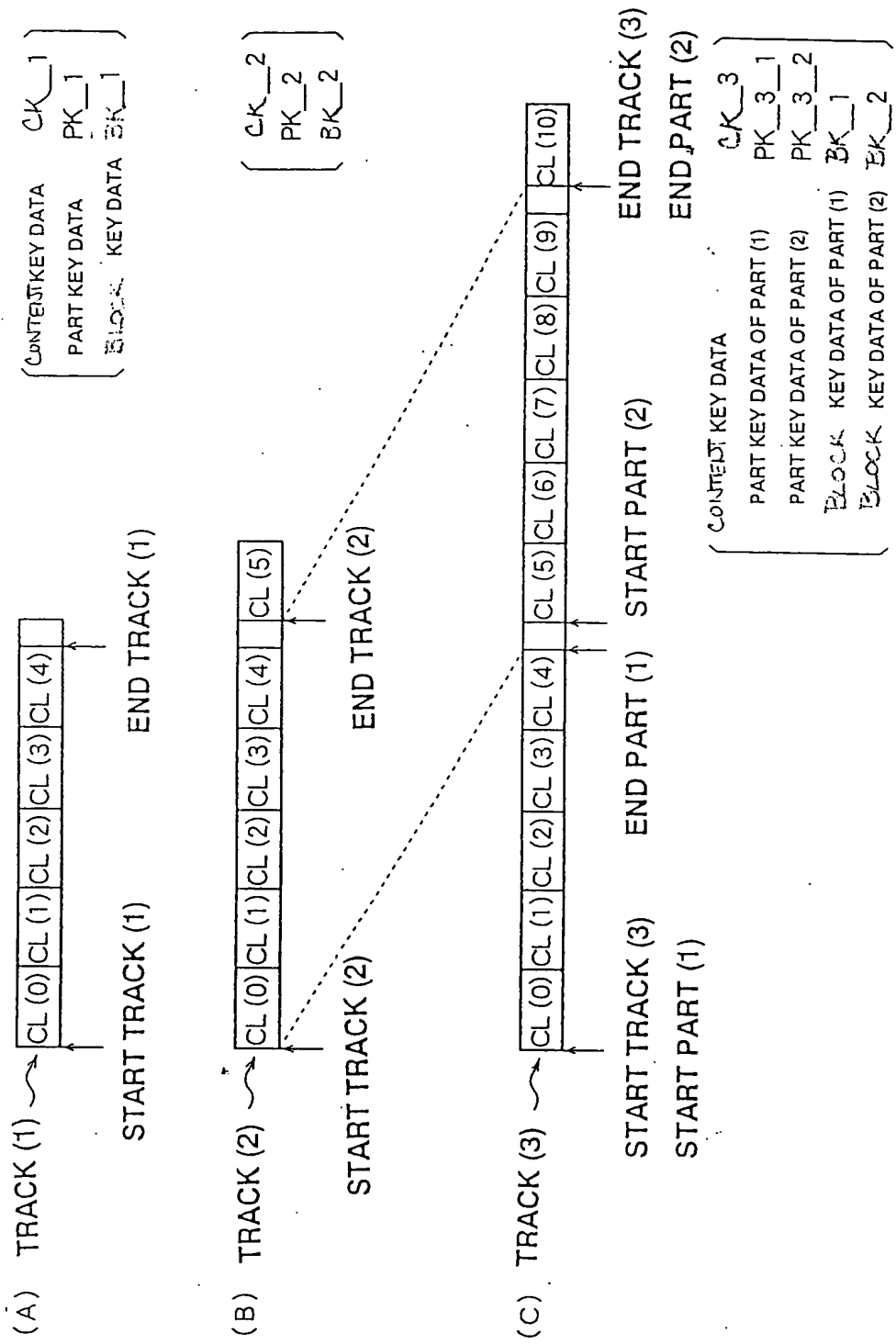


Figure 31



TRACK COUPLING PROCESSING

Figure 32

